Print Selection

Clear Cancel Print Print First Page

Section: Page(s): Print Copy: 1

Select?	Document ID	Section(s)	Page(s)	# Pages to print	Database
☑	20040069846	all	all	18	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	20040037410	all	all	24	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	20040034794	all	all	49	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	20040006541	all	all	10	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	20030159070	all	all	42	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	20020032661	all	all	11	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	6697806	all	all	* 93	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	6572014	all	all	16	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	6381626	all	all	11	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	6193153	all	all	16	PGPB,USPT,USOC,EPAB,JPAB,DWPI
☑	6092197	all	all	39	PGPB,USPT,USOC,EPAB,JPAB,DWPI

Note: Print requests for more than **49** pages are denoted by '*' and are in red.

Building	Room	Printer
cpk2	4c32	gbfrptr

Refine Search

Search Results -

Term	Documents
REPUTATION	2607
REPUTATIONS	199
(10 AND REPUTATION).PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD.	0
(L10 AND REPUTATION).PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD.	0

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L11

Refine Search

Recall Text | Clear | Interrupt

Search History

DATE: Wednesday, June 23, 2004 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L11	l10 and reputation	0	L11
L10	l1 and (response near authorization near user$)	22	L10
L9	l1 and (response near authorization)	225	L9
L8	l1 and (reputation near information)	7	L8
L7	L6 and ("authorization user")	13	L7
L6	L5 and community	113	L6
L5	L4 and database	114	L5
L4	L3 and activit$	114	L4
L3	L2 and reputation	117	L3

L2	authorization near user	3256	L2
L1	authoriz$ near user$	16004	L1

END OF SEARCH HISTORY

First Hit

Generate Collection Print

L10: Entry 4 of 22 File: PGPB Jan 8, 2004

DOCUMENT-IDENTIFIER: US 20040006541 A1
TITLE: Method and system for purchasing broadcast content

CLAIMS:

16. A method of providing broadcast music to users including the steps of: broadcasting the music in a protected format; providing a rendering system which receives the music in a protected format and plays the music once without the user purchasing additional rights; allowing a user to identify music which the user wishes to purchase and to send a message indicating that desire; receiving the message with the identification of the music which the user wishes to purchase and sending an authorization to the user; in response to the authorization, the user's system allows the identified music to be played more than the once the music could otherwise be played.

18. A method including the steps of claim 16 wherein the step of sending an authorization to the user includes the identification of the user authorized to play the music.

L10: Entry 14 of 22 File: USPT Feb 24, 2004

DOCUMENT-IDENTIFIER: US 6697806 B1
TITLE: Access network authorization

Abstract Text (1):
An access communication system provides access between a user system and a plurality of communication networks. The plurality of communication networks provide services to a user in the user system. An access communication system includes a local database system and an access server that is connected to the user system and the plurality of communication networks. The local database system receives a user logon. The local database system then processes the user logon to determine if the user is allowed access to the access communication system based on a local database system. The local database system then provides access to the access communication system to the user in response to the determination that the user is allowed access based on the local database system. The local database system then generates an authorization query for a second database system external to the local database system in response to the determination that the user is not allowed access based on the local database system. The local database system receives and processes an authorization response indicating whether the user is allowed to use the access system from the second database system. The local database system then provides access to the access communication system to the user in response to the authorization response that allows the user to use the access communication system.

Brief Summary Text (27):
In another aspect of the inventions for global authentication and access card, the database system receives a user logon. The database system then processes the user logon to determine if the user is allowed access to the access communication system based on a local database system. The database system then provides access to the access communication system to the user in response to the determination that the user is allowed access based on the local database system. The database system then generates an authorization query for a second database system external to the local database system in response to the determination that the user is not allowed access based on the local database system. The database system receives and processes an authorization response indicating whether the user is allowed to use the access system from the second database system. The database system then provides access to the access communication system to the user in response to the authorization response that allows the user to use the access communication system.

Detailed Description Text (9):
FIG. 6 depicts an access network in an example of the invention. The access network 520 comprises the database system 522, the access server 524, the firewall/router 526, the firewall/router 556, and the access server 554. The database system 522 comprises a local database system 570, a Lightweight Directory Access Protocol (LDAP) interface system 571, a central database system 580, a local database system 590, and an LDAP interface system 591. The local database system comprises a user profile system 572, an audit database system 573, a cache database system 574, a host system 575, a security server 576, a user authorization system 577, an alias translation system 578, and a personal DNS system 579. The central database system 580 comprises a user authorization system 581, a financial interface 582, and a

cross connect system 583. The local database system 590 comprises a user profile system 592, a user authorization system 593, and an availability system 594.

Detailed Description Text (67):
In one embodiment, the database system 522 uses a user authorization system 575 for checking if the user is known in the local database system 570. The user authorization system 575 contains all the prepaid customers, prepaid customer information, prepaid account codes, and the amount/quantity remaining in the prepaid account to verify if access is allowed. In one embodiment, the database system 522 uses a user authorization system 581 as the appeal server for checking if the user is known in the local database system 580. The user authorization system 581 contains all the prepaid customers, prepaid customer information, and the amount/quantity remaining in the prepaid account.

Detailed Description Text (78):
If there is foreign network account information, the database system 522 identifies the local database system 590 based on the foreign network account information and generates an authorization query for the local database system 590 in step 2214. The database system 522 then checks if the user is authenticated and authorized by the local database system 590 in step 2216. If the user is authenticated and authorized, the database system 522 logs contract and settlements information returned by the local database system 590 or indicated by the database system 522 in relation to local database system 590 in step 2218 before proceeding to step 2208. If the user is not known, the database system 522 proceeds to step 2212. In one embodiment, the local database system 570 uses the user authorization system 575 to check if the user is known in the local database system 570. In one embodiment, the local database system 590 uses the user authentication system 593 for authentication and authorization.

Detailed Description Text (83):
If the user is not native, the database system 522 checks if there is an authentication/authorization server in the database system 522 for a foreign network for user authentication in step 1910. If there is no authentication/authorization server in the database system 522 for the foreign network, the database system 522 transmits an instruction to the access server 524 to refuse the user logon and to disconnect the network device 512 from the access server 524 in step 2412 before returning to step 2402. If there is an authentication/authorization server in the database system 522 for the foreign network, the database system 522 generates an authorization query for the central database system 580 in step 2414. The database system 522 then checks if the user is known in the central database system 580 in step 2414. If the user is known, the database system 522 proceeds to step 2408. If the user is not known, the database system 522 proceeds to step 2410. In one embodiment, the central database system 580 uses a user authorization system 581 to check if the user is known.

Detailed Description Text (191):
If access control is allowed, the access server 524 generates and transmits an access control instruction to the database system 522 in step 4712. The database system 522 then receives and processes the access control instruction. The database system 522 identifies, authenticates, and authorizes the user and the requesting access server using the packet and path in step 4720. The database system 522 then retrieves the user access profile and the network device profile in step 4722. The database system 522 then checks if access control is allowed for the user and the network device based on the user access profile and the network device profile in step 4724. If access is not allowed, the database system 522 proceeds to step 4716.

CLAIMS:

1. A method of operating an access system including an access server to provide

access between a user system and a plurality of communication networks that provide services to a user, the method comprising: receiving a user logon into the access server; processing the user logon to determine if the user is allowed access to the access system based on a local database system; providing access to the access system to the user in response to the determination that the user is allowed access based on the local database system; generating an authorization query for a second database system external to the local database system in response to the determination that the user is not allowed access based on the local database system; in the second database system, receiving and processing the authorization query to determine whether the user is allowed access; in the second database system, generating and transmitting an authorization response to the local database system; receiving and processing the authorization response indicating whether the user is allowed to use the access system from the second database system; and providing access to the access system to the user in response to the authorization response that allows the user to use the access system.

10. An access system for providing access between a user system and a plurality of communication networks that provide services to a user, the access system comprising: an access server connected to the user system and the plurality of communication networks and configured to receive and transmit a user logon from the user system to a local database system; the local database system connected to the access server and configured to receive the user logon, process the user logon to determine if the user is allowed access to the access system based on the local database system, provide access to the access system to the user in response to the determination that the user is allowed access based on the local database system, generate an authorization query for a second database system external to the local database system in response to the determination that the user is not allowed access based on the local database system, receive and process an authorization response indicating whether the user is allowed to use the access system from the second database system, and provide access to the access system to the user in response to the authorization response that allows the user to use the access system; and the second database system connected to the local database system and configured to receive and process the authorization query to determine whether the user is allowed access and generate and transmit the authorization response for the local database system.

19. A software product for providing access between a user system and a plurality of communication networks that provide services to a user, the software product comprising: database software operational when executed by a processor to direct the processor to receive the user logon, process the user logon to determine if the user is allowed access to an access system based on a local database system, provide access to the access system to the user in response to the determination that the user is allowed access based on the local database system, generate an authorization query for a second database system external to the local database system in response to the determination that the user is not allowed access based on the local database system, receive and process an authorization response indicating whether the user is allowed to use the access system from the second database system, and provide access to the access system to the user in response to the authorization response that allows the user to use the access system; and a software storage medium operational to store the database software.

First Hit

Generate Collection Print

L10: Entry 2 of 22 File: PGPB Feb 26, 2004

DOCUMENT-IDENTIFIER: US 20040037410 A1
TITLE: Caller control of internet call waiting

Summary of Invention Paragraph:
[0011] In an embodiment, the interrupt code may be assigned different levels of authority for interrupting ICW and the data connection. Similarly, in another embodiment, the interrupt code may be assigned different levels of authority for disabling ICW and the data connection. For example, Calling Party Mom (i.e., a calling party that is a mother) may have an interrupt code that always allows interruption or disabling of the ICW and data connection (i.e., no authorization from user required). However, Calling Party Child (i.e., a calling party that is a child) may have an interrupt code that sends the notification message that Calling Party Child is trying to place an incoming call and prompts the user of the computer system to accept or to enter an authorization code in order to interrupt or to disable ICW and/or the data connection. If the user of the communications device does not accept or enter the authorization code or if the user fails to respond to the verification prompt within a selected period of time, then the telecommunications network may default to interrupt or to disable ICW and/or the data connection.

Brief Description of Drawings Paragraph:
[0019] FIG. 5 is a schematic showing user authorization to disable the ICW session and the active data connection as shown in the telecommunications system of FIG. 2;

Brief Description of Drawings Paragraph:
[0022] FIG. 8 is a schematic showing user authorization to disable the ICW session and the active data connection as shown in the telecommunications system of FIG. 6;

Detail Description Paragraph:
[0037] In an embodiment, the ICW Management Module 110 is used to establish a Caller Control of ICW Services Profile. The ICW DataServer 250 stores a database of Caller Control of ICW Services Profiles 252. The customer interacts with the ICW Management Module 110 and with Intranet 265 to access and login to the ICW DataServer 250 and to establish a profile in the database of Caller Control of ICW Services Profiles 252. The Caller Control of ICW Service Profile 255 could contain a variety of fields and/or files associated with at least one of the following: an authorized calling party's telephone number (e.g., a telephone number associated with a cellular phone of a parent or a customer, etc.), the customer's ISP login information, ISP password, a static IP address (if applicable), preferences for interrupting or disabling (e.g., always automatically disable ICW and data connection, always automatically interrupt ICW and data connection, prompt caller for selection to interrupt or disable, etc.), preferences for sending a notification message to the computer system 100 prior to interrupting or disabling (e.g., always send notification message prior to disabling, never send notification message prior to interrupting, prompt caller for selection of notification message, etc.), and preferences for requesting an authorization code back from a user of the computer system 100 prior to interrupting or disabling (e.g., always prompt user for authorization, only prompt user for authorization if calling party wants to

disable, etc.).

Detail Description Paragraph:
[0043] FIG. 5 illustrates a telecommunications system 500 similar to the telecommunications system disclosed in FIG. 4. In particular, telecommunications system 500 includes an authorization response 510 from the user of computer system 100 prior to disabling ICW and the data connection. The authorization response 510 might be most useful when different levels of authority for disabling ICW and the data connection are associated with the interrupt code. For example, Calling Party Mom may have an interrupt code that always allows disabling of the ICW and data connection. However, Calling Party Child may have an interrupt code that sends the disable notification message 410 to computer system 100 identifying that Calling Party Child is trying to place an incoming call. The disable notification message 410 prompts the user of computer system 100 to accept or to enter an authorization code in order to disable ICW and the data connection. If the user of the computer system 100 does not accept or enter the authorization response or if the user fails to respond to the authorization prompt within a selected period of time, then the PSTN 245 may default to disable ICW and the data connection. The PSTN 245 could, alternatively, default and not disable the data connection when the user fails to respond to the authorization prompt.

Detail Description Paragraph:
[0053] The method continues with FIG. 12. If cancellation/disconnection is selected, the telecommunications network determines whether a notification message should be sent to the communications device (block 1210). If no notification message is to be sent, then the telecommunications network cancels the ICW session and data connection (block 1220) and connects the incoming call to the called telephone number (block 1230). If the telecommunications network determines that the notification message should be sent, then a computer system application (e.g., ICW Management Module as shown as reference numeral 110 in FIGS. 1-10) is queried for a dynamic IP address (block 1240), and the telecommunications network (via telecommunications switch) or the data network (via gateway) communicates the notification message to the communications device via the IP address (block 1250). The notification message is played by the communications device to alert the called party of the incoming call (not shown), and, thereafter, the telecommunications network determines whether the customer or user should authorize caller control of the ICW session and data connection (block 1260). If so, then the telecommunications network or data network prompts for and receives an authorization response (block 1270), disables ICW and data connection (block 1220), and connects the incoming call to the called telephone number (block 1230). If not, then the telecommunications network disables ICW and data connection (block 1220) and connects the incoming call to the called telephone number (block 1230).

Detail Description Paragraph:
[0054] FIG. 13 illustrates interruption/suspension. If interruption/suspension is selected, the telecommunications network queries the computer system software (e.g., ICW Management Module reference numeral 110 as shown in FIGS. 1-10) for a dynamic IP address (block 1310) and determines whether a notification message should be sent to the communications device (block 1320). If no notification message is to be sent, then the telecommunications network interrupts/suspends the ICW session and data connection to connect the incoming call via the IP address (block 1360). If the telecommunications network determines that the notification message should be sent, then the telecommunications network (via telecommunications switch) or the data network (via gateway) communicates the notification message to the communications device via the IP address (block 1340). The notification message is played by the communications device to alert the customer or user of an incoming call (not shown), and, thereafter, the telecommunications network determines whether the customer or user should authorize caller control of the ICW session and data connection (block 1340). If so, then the telecommunications network or data network prompts for and receives an authorization response (block 1350) and

connects the incoming call to the communications device via IP address (block 1360). If not, then the telecommunications network or data network connects the incoming call to the communications device without prompting for authorization (block 1360).

L10: Entry 19 of 22 File: USPT Feb 27, 2001

DOCUMENT-IDENTIFIER: US 6193153 B1
TITLE: Method and apparatus for non-intrusive biometric capture

Brief Summary Text (4):
With the wide-spread use of computers and the Internet, the security of data stored within computers is of increasing concern. Many methods have been devised to restrict the access of computer data or applications to authorized users, such as installing computer firewalls, implementing complex password schemes, using call-back numbers, providing challenge and response hardware, and the like. As illustrated regularly in the popular press, for each such protection mechanism, hackers have found many ways to circumvent them.

Brief Summary Text (8):
Another drawback to present biometric capture devices include that they are typically stand-alone devices having virtually no function other than capturing the biometric data. Because such devices are stand-alone, they are typically only used as gate keeper devices. As a result, when the biometric security device has been satisfied, fulfilled, or bypassed, there is open access to the secure data, the secure area, and the like. For example, once a user has been authorized to enter a security door, the door may be left open for unauthorized users to enter, similarly, when a screen saver password has been entered correctly, the files on the computer may be accessed.

Detailed Description Text (89):
In one embodiment of the present invention, a application program such as an on-line financial transaction, or a secure communication program may periodically require capturing and processing of biometric data from the user. The biometric data may be embedded in a response or an authorization by the user, or relayed to another computer on the network for archival, verification, and the like.

First Hit

Generate Collection Print

L10: Entry 12 of 22 File: PGPB Mar 14, 2002

DOCUMENT-IDENTIFIER: US 20020032661 A1
TITLE: Method for the authorization of transactions

Summary of Invention Paragraph:
[0011] It is proposed that a check is performed whether the authorization request comprises a string and the indication is the detected string or a default string else. The string contains preferably a short text which identifies the content for authorization to the user in a clear way. It can, for example, comprise a reference text describing the content for authorization or a short reference to the content as a whole like a document number or contract number. For orders and purchases, a short description and the number of selected items, the amount for each item and the total amount to be paid are suitable elements of the string. A default string is preferably a general information that a transaction is to be authorized, optionally with a warning that an approval constitutes a completion of a contract. It is possible that the user equipment has a stored set with several default strings which are displayed according to parameters in the authorization request.

Summary of Invention Paragraph:
[0021] A server for processing authorization procedures in a communication system has an interface to exchange messages with user equipment of the communication system. Generally, messages are relayed by further devices in the communication system, e.g. routers forwarding the messages or radio base stations providing a wireless connection to the user equipment. The server has a processing system with a unit to send an authorization request for a content which is to be authorized to the user equipment and to receive an authorization response from the user equipment. Preferably, the unit is a software program.

Detail Description Paragraph:
[0043] The authorization response from the user equipment UE comprises the binary identifier H signed by the user equipment UE, i.e. SO (ck, H) wherein ck is an authorization key of the user equipment UE. The value SO (ck, H) ensures that the authorization request was signed by the user equipment and identifies clearly the signed content. Optionally, a signed receipt containing a concatenation of the value which is to be signed and the text string for display can be demanded by the server, e.g. by the parameter "receipt" in FIG. 2. Storing the receipts by the server provides for a repudiation of the signed transaction content by the user in case of future disputes about the signed content. The receipt provides a proof that the user was informed about the content of the signed data.

Detail Description Paragraph:
[0052] If a user wants, for example, to purchase a plane ticket with a credit card, he starts a browser application on his user equipment, browses to the WAP site of a travel agency and exchanges messages to select a flight, date and seat. The user selects a protocol for the purchase, e.g. the Secure Electronic Transaction protocol, and sends a service request with the selected items to the mobile server MS. Optionally, the request contains further information, e.g. a selected merchant if several merchants share the further server FS. The mobile server MS initiates the payment transaction with the further server FS by a payment initiation request forwarding the selection of the user. The further server replies with a payment initiation response message which comprises authentication certificates of the

supplier and a content which has to be authorized by the user, generally a contract or a part of a contract like an amount for a purchase. In the example, the content preferably comprises the selected flight, date and seat together with the amount for the ticket.

CLAIMS:

14. Server for processing authorization procedures in a communication system with an interface to exchange messages with user equipment of the communication system, wherein the server has a processing system adapted to send an authorization request for a content which is to be authorized to the user equipment and to receive an authorization response from the user equipment, characterized in that the processing system determines an identifier (H) for the content and includes the identifier (H) into the authorization request, the processing system determines an indication for the content and includes the indication into the authorization request and the server (MS) checks the authorization response for the identifier (H) signed by the user equipment (UE).

First Hit

Generate Collection Print

L10: Entry 1 of 22 File: PGPB Apr 15, 2004

DOCUMENT-IDENTIFIER: US 20040069846 A1
TITLE: Method and apparatus for non-intrusive biometric capture

Summary of Invention Paragraph:
[0004] With the wide-spread use of computers and the Internet, the security of data stored within computers is of increasing concern. Many methods have been devised to restrict the access of computer data or applications to authorized users, such as installing computer firewalls, implementing complex password schemes, using call-back numbers, providing challenge and response hardware, and the like. As illustrated regularly in the popular press, for each such protection mechanism, hackers have found many ways to circumvent them.

Summary of Invention Paragraph:
[0008] Another drawback to present biometric capture devices include that they are typically stand-alone devices having virtually no function other than capturing the biometric data. Because such devices are stand-alone, they are typically only used as gate keeper devices. As a result, when the biometric security device has been satisfied, fulfilled, or bypassed, there is open access to the secure data, the secure area, and the like. For example, once a user has been authorized to enter a security door, the door may be left open for unauthorized users to enter, similarly, when a screen saver password has been entered correctly, the files on the computer may be accessed.

Detail Description Paragraph:
[0115] In one embodiment of the present invention, a application program such as an on-line financial transaction, or a secure communication program may periodically require capturing and processing of biometric data from the user. The biometric data may be embedded in a response or an authorization by the user, or relayed to another computer on the network for archival, verification, and the like.

L10: Entry 16 of 22 File: USPT Jun 3, 2003

DOCUMENT-IDENTIFIER: US 6572014 B1
TITLE: Method and apparatus for non-intrusive biometric capture

Brief Summary Text (4):
With the wide-spread use of computers and the Internet, the security of data stored within computers is of increasing concern. Many methods have been devised to restrict the access of computer data or applications to authorized users, such as installing computer firewalls, implementing complex password schemes, using call-back numbers, providing challenge and response hardware, and the like. As illustrated regularly in the popular press, for each such protection mechanism, hackers have found many ways to circumvent them.

Brief Summary Text (8):
Another drawback to present biometric capture devices include that they are typically stand-alone devices having virtually no function other than capturing the biometric data. Because such devices are stand-alone, they are typically only used as gate keeper devices. As a result, when the biometric security device has been satisfied, fulfilled, or bypassed, there is open access to the secure data, the secure area, and the like. For example, once a user has been authorized to enter a security door, the door may be left open for unauthorized users to enter, similarly, when a screen saver password has been entered correctly, the files on the computer may be accessed.

Detailed Description Text (89):
In one embodiment of the present invention, a application program such as an on-line financial transaction, or a secure communication program may periodically require capturing and processing of biometric data from the user. The biometric data may be embedded in a response or an authorization by the user, or relayed to another computer on the network for archival, verification, and the like.

CLAIMS:

8. The method of claim 1 further comprising determining whether the user is authorized to run the first program in response to the biometric data signals from the user; and thereafter inhibiting the first program from running when the user is not authorized to run the first program.

9. A method for providing in-session authentication of users with a computer system comprises: sending a series of signals to a user input device to initiate biometric capture with the user input device; receiving biometric data of a user from the user input device in response to the series of signals; determining an identity of the user in response to the biometric data; determining whether the user is authorized to begin a user-session in response to the identity of the user; initiating the user-session when the user is authorized to begin the user-session; thereafter during the user-session the method includes: sending an additional series of signals to the user input device to initiate biometric capture with the user input device; receiving biometric data of a current user of the user input device from the user input device in response to the additional series of signals; determining an identity of the current user in response to the biometric data; and storing the identity of the current user in a user log; wherein the user-session is

maintained while determining the identity of the current user and while storing the identity of the current user.

11. The method of claim 10 further comprising restoring the user-session when the current user is authorized to maintain the user-session.

16. The method of claim 9 further comprising terminating the user-session when the current user is not authorized to maintain the user-session.

17. An computer program product for a computer system for authenticating a user during a computer system session including a processor comprises: code that directs the processor to receive event data of a user from a user input device; code that directs the processor to send a series of signals to the user input device to initiate biometric capture with the user input device; code that directs the processor to receive biometric data of the user from the user input device in response to the series of signals; code that directs the processor to determine an identity of the user in response to the biometric data; code that directs the processor to determine whether the user is authorized to begin a user-session in response to the identity of the user; code that directs the processor to initiate the user-session when the user is authorized to begin the user-session; thereafter during the user-session; code that directs the processor to send an additional series of signals to the user input device to initiate biometric capture with the user input device; code that directs the processor to receive biometric data of current user of the user input device from the user input device in response to the additional series of signals; and code that directs the processor to determine an identity of the current user in response to the biometric data; wherein the codes reside on a tangible media; wherein the user-session is maintained while determining the identity of the current user.

23. The computer program product of claim 17 further comprising code that directs the processor to determine whether the current user is authorized to maintain the user-session in response to the identity of the current user; and code that directs the processor to terminate the user-session if the current user is not authorized to maintain the user-session.

L10: Entry 20 of 22 File: USPT Jul 18, 2000

DOCUMENT-IDENTIFIER: US 6092197 A
TITLE: System and method for the secure discovery, exploitation and publication of information

Detailed Description Text (9):
thus prompt the user 7 to provide information, such as personal, secret or confidential information, "private facts," and upon receiving such private facts, determine whether additional prompts should be provided to the user 7 to obtain additional private facts, and what the content of such additional prompts should be. Therefore, during the execution of the dialog classes, as further described, the user 7 can be asked to disclose certain private facts, such as, for example, date of birth, social security number, annual income, mother's maiden name, other family information, eye and hair color, and user-preferences. Execution of the dialog classes enables the user 7 to authorize certain private facts to be made available and published as public facts. Public facts are thus private facts made available to the sender 4 only in response to authorization by the user 7. Additionally, public facts can further comprise sender-related data such as, for example, service messages. In the present embodiment, the interface computer 5 can therefore store, modify and retrieve private and public facts relative to the user 7 as well as public facts relative to the sender 4.

Detailed Description Text (10):
Therefore, the interface computer 5 receives the dialog classes from memory module 1', executes the dialog classes and interacts with the user 7. Any information provided by the user 7 in response to such interactions is stored in the memory module 6 as private facts. These private facts remain in the memory module 6 and are copied as outbound public facts only in response to authorization by the user 7 for disclosure to the sender 4, as will be further described. The outbound public facts are stored in memory module 8. As described above, system information or public facts previously provided by the user 7 to the sender 4, or simply provided by the sender 4, are stored in memory module 9 as inbound public facts, and are transmitted to the interface computer 5 to aid in allowing appropriately tailored prompts to be directed to the user 7.

Detailed Description Text (40):
Referring to FIG. 6D, another rule for processing a publishing request is described. Unlike the rules described above in FIGS. 6B and 6C, this rule is a pure rule 150, that is, the request is automatically fulfilled without requiring user authorization. In this rule, authorization is not required because the fact has previously been published by the user 7, and execution of this rule simply fulfills the publishing request by providing the most recent value of the public fact 8 to the sender 4. That is, a version of the public fact was given, and a new or updated version is requested by the sender 4. This rule also has a priority R-p 216 of 11. The condition R-c 218 associated with this rule requires that the publishing request list 60 comprise a public fact 8 to be updated, and that the name 61 of the first element of the list 60 is listed as the name 64 in an entry in the hash table 63. As described above, this signifies that some attempt to publish it has already been made. Additionally, the permission status 65 corresponding to the name 64 must be equal to "authorized," that is, the user 7 previously authorized disclosure of the public fact to a sender 4. The conclusion RR-c 220 associated with this rule

updates the entry in the hash table 63 with the name 64 equal to the name 61 in the publishing request list 60 by making the conclusion date of last access 66 equal to the current date of the interface computer 5. Then the conclusion RI-c 220 sets the value 67 equal to the value 62 in the publishing request list 60. Finally, the conclusion RI-c 220 removes the first element off the list 60, again, so that the DEP 14 can process the next request.

Detailed Description Text (46):
Referring to FIG. 6E, authorization cancellation can be implemented by a fourth pure rule with the DEP 14. In this embodiment, a rule having a priority R-p 222 of 11 allows a user to cancel previously given authorizations to publish private facts. The condition R-c 224 associated with the rule can be that a time period has elapsed or that a special request has been set. A time period can be, for example, a month or a quarter of the year. For time-sensitive private facts, those being private facts that are quickly subject to change, the time period can be significantly shorter, such as, for example, a week. The expiration of the time period can be measured through the use of a clock or "chronometer" object which can access the current date with the desired accuracy and determine the amount of time that has elapsed since initialization of the date. In this manner, regular checks can be made on a user's authorization to disclose a private fact 6. A special request can be, in the present embodiment, an affirmative step taken by the user 7 to initiate cancellation of previously given authorizations. An affirmative step can be signaled for example, by the user 7 clicking on an icon or touching an icon on a touchscreen, which represents an authorization for cancellation. As shown, the conclusion 226 resets the authorization time as well as the authorization cancellation request, obtains the current date, updates each entry in the outbound public facts table 63 with permission status 65 "authorized" to "denied", and changes the date of last access 66 to the current date. In this manner, the private facts previously authorized for publication are no longer available as public facts. While the rule in the present embodiment issues a blanket denial of previously given authorizations, in other embodiments, the system can use a plurality of similar rules with more specific targets for cancellation of only certain authorizations.